UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN RE GEICO CUSTOMER DATA BREACH LITIGATION	Case No. 21-CV-2210-KAM-SJB

PLAINTIFFS' OPPOSITION TO DEFENDANTS' MOTION TO DISMISS

TABLE OF CONTENTS

INTRODUCTION 1

RULE 12(b)(1) AND 12(b)(6) LEGAL STANDARDS 4

ARGUMENT 5

I. PLAINTIFFS SATISFY THE REQUIREMENTS FOR ARTICLE III STANDING 5

A. GEICO's Use and Disclosure of Plaintiffs' PI Caused Article III Injury-In-Fact. 5

B. Efforts to Mitigate Existing Identity Theft Constitute Injuries-in-Fact 8

C. "Certainly Impending" Risk of Identity Theft Constitutes an Injury-in-Fact 11

D. Plaintiffs' Injuries Are Fairly Traceable to the Data Disclosure and Likely to be Redressed by a Favorable Judicial Decision 14

II. PLAINTIFFS ADEQUATELY PLEAD THAT GEICO VIOLATED THE DPPA 15

A. GEICO Knowingly Disclosed Plaintiffs' Protected Driver's License Numbers to Unauthorized Third Parties 16

B. Plaintiffs Allege That GEICO Obtained PI from a Motor Vehicle Record 19

C. GEICO Did Not Disclose Plaintiffs' Driver's License Numbers to Unauthorized Third Parties for a Proper Purpose Under the DPPA 22

D. GEICO Did Not Use Reasonable Care in Disclosing PI to Third Parties 26

III. PLAINTIFFS STATE A CLAIM FOR NEGLIGENCE 28

A. GEICO Breached a Duty of Care Owed to Plaintiffs 28

B. GEICO's Breach Proximately Caused Plaintiffs' Legally Cognizable Injuries 30

IV. PLAINTIFFS STATE A CLAIM FOR NEGLIGENCE PER SE 31

V. PLAINTIFFS STATE A GBL § 349 CLAIM 33

VI. PLAINTIFFS ARE ENTITLED TO DECLARATORY AND INJUNCTIVE RELIEF 35

VII. CONCLUSION 36

TABLE OF AUTHORITIES

Cases **Pages(s)**

Allen v. Vertafore, Inc.,
4:20-cv-04139, 2021 WL 3148870 (S.D. Tex. June 14, 2021) *report and recommendation adopted,* No. 4:20-CV-04139, 2021 WL 3144469 (S.D. Tex. July 23, 2021), *aff'd,* 28 F.4th 613 (5th Cir. 2022), *cert. denied sub nom. Allen v. Vertavore, Inc.,* No. 21-1555, 2022 WL 4652002 (U.S. Oct. 3, 2022 .....8, 18

Bans Pasta, LLC v. Mirko Franchising, LLC,
No. 7-13-cv-00300-JCT, 2014 WL 637762 (W.D. Va. Feb. 12, 2014).....33

Barrows v. Becerra, 24 F.4th 116 (2d Cir. 2022).....5

Baysal v. Midvale Indemnity Company,
No. 21-cv-394-WMC, 2022 WL 1155295 (W.D. Wis. Apr. 19, 2022).....10

Carter v. HealthPort Techs., LLC,
822 F.3d 47 (2d Cir. 2016) 14

Coastline Terminals of Connecticut, Inc. v. USX Corp.,
156 F. Supp. 2d 203 (D. Conn. 2001).....31

Cohen v. Ne. Radiology, P.C.,
No. 20-cv-1202-VB, 2021 WL 293123 (S.D.N.Y. Jan. 28, 2021) 33, 34

Colpitts v. Blue Diamond Growers,
527 F. Supp. 3d 562 (S.D.N.Y. 2021) 4

Cooper v. Slice Techs., Inc.,
No. 17-CV-7102 (JPO), 2018 WL 2727888 (S.D.N.Y. June 6, 2018).....6

Corbin v. Wilson,
No. 10-CV-3156 NGG RER, 2011 WL 4374213 (E.D.N.Y. Aug. 26, 2011) *report and recommendation adopted,* No. 10-CV-3156 NGG RER, 2011 WL 4381152 (E.D.N.Y. Sept. 19, 2011) 32

Cowan v. Ernest Codelia, P.C.,
No. 98-cv-5548-JGK, 2001 WL 856606 (S.D.N.Y. July 30, 2001).....16

Dahlstrom v. Sun-Times Media, LLC,
777 F.3d 937 (7th Cir. 2015) 25, 26

Doe v. Uber Techs., Inc.,
551 F. Supp. 3d 341 (S.D.N.Y. 2021) 34

Elliott v. City of New York,
95 N.Y.2d 730 (2001).....31

Enslin v. The Coca-Cola Company,
136 F.Supp.3d 654 (E.D. Pa. 2015) 16, 18

Fagan v. AmerisourceBergen Corp.,
356 F. Supp. 2d 198 (E.D.N.Y. 2004) 32

Fero v. Excellus Health Plan Inc.,
236 F. Supp. 3d 735 (W.D.N.Y. 2017), *on reconsideration*, 304 F. Supp. 3d 333 (W.D.N.Y. 2018), *and order clarified*, 502 F. Supp. 3d 724 (W.D.N.Y. 2020) 35

Garey v. James S. Farrin, P.C.,
35 F.4th 917 (4th Cir. 2022) 6, 7, 21

Gordon v. Softech Int'l,
726 F.3d 42 (2d Cir. 2013) ..... *passim*

Greenstein v. Noblr Reciprocal Exchange,
No. 21-cv-04537-JSW, 2022 WL 472183 (N.D. Cal. Feb. 15, 2022) 10

Gulsvig v. Mille Lacs County,
No. CIV. 13-1309 JRT/LIB, 2014 WL 1285785 (D. Minn. Mar. 31, 2014) 18

In re Anthem, Inc. Data Breach Litig.,
162 F. Supp. 3d 953 (N.D. Cal. 2016) 35

In re Cap. One Consumer Data Sec. Breach Litig.,
488 F. Supp. 3d 374 (E.D. Va. 2020) 31, 32, 35, 36

In re Equifax, Inc., Customer Data Security Litig.,
362 F. Supp. 3d 1295 (N.D. Ga. 2019) 29, 31, 33

In re GE/CBPS Data Breach Litig.,
No. 20-cv-2903-KPF, 2021 WL 3406374 (S.D.N.Y. Aug. 4, 2021) 12, 29, 30, 31

In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.,
440 F. Supp. 3d 447 (D. Md. 2020) 33

In re Rutter's Inc. Data Sec. Breach Litig.,
511 F. Supp. 3d 514 (M.D. Pa. 2021) 29

In re USAA Data Sec. Litig.,
No. 21-cv-5813-VB, 2022 WL 3348527 (S.D.N.Y. Aug. 12, 2022) ..... *passim*

John v. Whole Foods Mkt. Grp., Inc.,
858 F.3d 732 (2d Cir. 2017) 5

Lugo v. St. Nicholas Assocs.,
2 Misc. 3d 212 (Sup. Ct. N.Y. Cnty. 2003), *aff'd,* 795 N.Y.S.2d 227 (2005) 32

Lujan v. Defenders of Wildlife,
504 U.S. 555 (1992) 5

Mallak v. Aitkin Cnty.,
9 F. Supp. 3d 1046 (D. Minn. 2014) 15

Maracich v. Spears,
570 U.S. 48 (2013) 7, 15, 22

McDonough v. Anoka County,
799 F.3d 931 (8th Cir. 2015) 18

McFarlane v. Altice USA, Inc.,
524 F. Supp. 3d 264 (S.D.N.Y. 2021) 15

McKenzie v. Allconnect, Inc.,
369 F. Supp. 3d 810 (E.D. Ky. 2019) 29

McMorris v. Carlos Lopez & Associates, *LLC*,
995 F.3d 295 (2d Cir. 2021) 11, 12, 13, 14

MedImmune, Inc. v. Genentech, Inc.,
549 U.S. 118 (2007) 35

Mount v. PulsePoint, Inc.,
684 F. App'x 32 (2d Cir. 2017)*, as amended* (May 3, 2017) 6

Orlander v. Staples, Inc.,
802 F.3d 289 (2d Cir. 2015) 33

Park v. Am. Fam. Life Ins. Co.,
No. 22-cv-171-WMC, 2022 WL 2230171 (W.D. Wis. June 17, 2022) 10

Pichler v. UNITE,
542 F.3d 380 (3d Cir. 2008) 17, 22, 24

Remijas v. Neiman Marcus Group, LLC,
794 F.3d 688 (7th Cir. 2015) 9, 12

Reno v. Condon,
528 U.S. 141 (2000) 20

Rudolph v. Hudson's Bay Co.,
No. 18-cv-8472-PKC , 2019 WL 2023713 (S.D.N.Y. May 7, 2019) 9

Sackin v. TransPerfect Global, Inc.,
278 F. Supp. 3d 739 (S.D.N.Y. 2017) 28

Sanchez v. Ehrlich,
No. 16-CV-8677 (LAP), 018 WL 2084147 (S.D.N.Y. Mar. 29, 2018) 33

Senne v. Vill. of Palatine, Ill.,
695 F.3d 597 (7th Cir. 2012) 16, 17, 22, 26

Spokeo, Inc. v. Robins,
578 U.S. 330 (2016)*, as revised* (May 24, 2016).....5, 6, 11, 14

Stone v. City of New York,
No. 05-cv-2736-SLT, 2009 WL 10705814 (E.D.N.Y. Dec. 30, 2009) 31

Susan B. Anthony List v. Driehaus,
573 U.S. 149 (2014).....11

Toretto v. Donnelley Fin. Sols., Inc.,
No. 1:20-cv-2667-GHW, 2022 WL 348412 (S.D.N.Y. Feb. 4, 2022) 28, 31

TransUnion LLC v. Ramirez,
141 S. Ct. 2190 (2021).....6, 8, 13

Uzuegbunam v. Preczewski,
141 S. Ct. 792 (2021).....14

Van Gaasbeck v. Webatuck Cent. Sch. Dist. No. 1,
21 N.Y.2d 239 (1967).....31

Welch v. Theodorides-Bustle,
677 F. Supp. 2d 1283 (N.D. Fla. 2010) 25

Whalen v. Michael Stores, Inc.,
153 F. Supp. 3d 577 (E.D.N.Y. 2015) 9, 10

Statutes

15 U.S.C. § 15 32

15 U.S.C. § 45 4

15 U.S.C. § 1681 *et seq* 6

15 U.S.C. § 6801 *et seq.* 4

18 U.S.C. § 2721(b)(6).....22, 23, 24, 25

18 U.S.C. § 2724, *et seq*. 1

18 U.S.C. § 2724(a).....7, 15, 16, 19

18 U.S.C. § 2724(b).....7

18 U.S.C. § 2721(a)(1) 22

18 U.S.C. § 2721(a)(2) 22

28 U.S.C. § 2201 35

N.Y. Gen. Bus. Law § 349. .....2, 34

N.Y. Gen. Bus. Law § 349(a). 33

Other Authorities

U.S. Const. art. III 5

Rules

Fed. R. Civ. P. 12(b)(1) 2, 3, 4

Fed. R. Civ. P. 12(b)(6) 2, 3, 4

Plaintiffs Michael Viscardi, Kathleen Dorety, and William Morgan (collectively, "Plaintiffs") submit this Memorandum in Opposition to Defendants' Motion to Dismiss ("Motion or "MTD") filed by Government Employees Insurance Company d/b/a GEICO, GEICO Casualty Company, GEICO Indemnity Company, and GEICO General Insurance Company (collectively, "GEICO" or "Defendants").

INTRODUCTION

Data means money. Corporations know this and are constantly finding new ways to leverage data to increase their profits, even at the expense of consumers' privacy. Driver's license numbers are particularly valuable. For insurance companies like GEICO, driver's license numbers are important—they can be used to identify potential customers and for myriad other business purposes. But, in the wrong hands, drivers' license numbers can be used to perpetrate a host of frauds, including unemployment and other benefits fraud. A driver's license number can be a critical part of building a fraudulent identity, and a forged driver's license, alone, can sell for hundreds of dollars.

To guard consumers against corporate temptations to use private driver's license information for commercial gain, Congress passed the Drivers' Privacy Protection Act, 18 U.S.C. § 2724, *et seq*. Among other things, the DPPA regulates the purposes for which private companies can obtain, use, and disclose driver's license numbers and other protected information ("PI"). While there are some legitimate purposes for which insurance companies may obtain, use, or disclose driver's license numbers, the DPPA does not permit doing so in order to increase insurance sales.

In what was nothing more than a profit-motivated business decision, GEICO disregarded the prohibitions of the DPPA. GEICO did so by knowingly adding a feature to its online insurance

quoting platform where an individual's driver's license number would be automatically displayed to anyone who entered a bare minimum of publicly available information about that individual into Defendant's sales website. This feature was added to speed up the insurance application and sales process, in the hope that a speedier process would increase sales volume for GEICO and thus improve its bottom line. In adding this unsecured feature to its website, GEICO broke the law by using and disclosing Plaintiffs' and class members' information for purposes not allowed by the law.

GEICO's decision did not go unnoticed by criminal harvesters of PI. Third parties mined GEICO's website to collect thousands of consumers' driver's license numbers, and to subsequently use those numbers to submit fraudulent applications for government benefits. GEICO's profit-driven decision exposed sensitive information that it was legally obligated to protect, and compromised Plaintiffs' and class members' privacy. Its misconduct and failures violated the DPPA, among other laws.

All Plaintiffs had their information exposed without authorization as a result of Defendant's decision. They seek redress for their injuries, individually and on behalf of all others similarly situated. The Consolidated Complaint ("Complaint" or "CAC") includes claims for violations of the DPPA, negligence, negligence per se, violations of the New York General Business Law ("GBL") § 349, invasion of privacy, and declaratory and injunctive relief.

GEICO has moved to dismiss Plaintiffs' claims, arguing under Rule 12(b)(1) that there is no standing and under Rule 12(b)(6) that Plaintiffs fail to assert a claim upon which relief can be granted. Each argument for dismissal fails, for reasons that have been exhaustively examined by other jurists in this Court applying New York and Second Circuit precedent. GEICO was not the only insurer to engage in this practice. Indeed, individuals asserting similar claims against United

Services Automobile Association ("USAA") recently defeated a nearly identical motion to dismiss. *See In re USAA Data Security Litigation*, No. 21-cv-5813-VB, 2022 WL 3348527 (S.D.N.Y. Aug. 12, 2022) ("*In re USAA*").

As the Court found in *In re USAA*, GEICO's Rule 12(b)(1) motion fails because Plaintiffs have alleged three independent bases for standing. *First,* GEICO's statutory violations of the DPPA invaded plaintiffs' privacy. This kind of invasion constitutes an intangible injury and is analogous to claims actionable at common law. It is therefore sufficient for Article III standing. *Second,* Plaintiffs have alleged tangible injury in the form of lost time expense incurred as a result of being targets of fraud that resulted from GEICO's disclosure. Plaintiffs make detailed allegations concerning their experience of actual fraud and their fraud mitigation efforts. *Third,* Plaintiffs have alleged imminent future injury. The data was stolen in a targeted attempt, was already used to perpetrate fraud, and is of a sufficiently sensitive nature as to pose an ongoing threat.

Defendants' Rule 12(b)(6) motion also fails, for multiple reasons also discussed in *In re USAA,* including the following: *First*, for the same reasons that Plaintiffs' allegations survive a 12(b)(1) motion, Plaintiffs' allegations are sufficient to confer Article III standing and survive a 12(b)(6) motion on that basis. *Second*, GEICO's voluntary decision to collect sensitive information, such as driver's license numbers, from state motor vehicle records and to use and disclose this information on its publicly available website for immediate and unfettered access by cybercriminals violated the DPPA. GEICO's arguments to the contrary largely mirror those rejected in *In re USAA* and are equally unavailing here. *Third*, Plaintiffs adequately plead that GEICO's decision to include the auto-population feature in its insurance quote process and failure to implement reasonable safeguards to ensure the appropriate function of that feature against

improper, potentially criminal use, constitutes a breach of the duty of reasonable care owed to Plaintiffs and class members. *Fourth*, Plaintiffs adequately plead that this alleged misconduct constitutes negligence per se under the Federal Trade Commission Act (15 U.S.C. § 45) ("FTC Act") and Gramm-Leach-Bliley Act (15 U.S.C. § 6801 *et seq.*) ("GBL"). *Finally*, the allegations show an ongoing, actionable dispute arising out of GEICO's continued collection, storage, and use of Plaintiffs' and class members' sensitive personal data, as well as inadequate data-security measures, all of which constitute a concrete harm that cannot be remedied solely with monetary damages. Accordingly, Plaintiffs' and class members are entitled to declaratory and injunctive relief. For these reasons and all of those that follow, GEICO's Motion should be denied in its entirety.

RULE 12(b)(1) AND 12(b)(6) LEGAL STANDARDS

A facial challenge to standing under Fed. R. Civ. P. 12(b)(1) and a motion to dismiss for failure to state a claim under Fed. R. Civ. P. 12(b)(6) use the same standard: all well-pleaded factual allegations must be accepted as true, and the court draws all reasonable inferences from those allegations in favor of the plaintiff. *See Colpitts v. Blue Diamond Growers*, 527 F. Supp. 3d 562, 574 (S.D.N.Y. 2021). A motion to dismiss should be denied where a complaint contains sufficient factual matter that plausibly alleges the elements of standing or the elements of the claims. *Id.*[1]

[1] The only difference is that on a Rule 12(b)(1) motion, a plaintiff "bears the burden of proving that subject matter jurisdiction exists by a preponderance of the evidence." *Colpitts v. Blue Diamond Growers*, 527 F. Supp. 3d 562, 574 (S.D.N.Y. 2021).

ARGUMENT

I. PLAINTIFFS SATISFY THE REQUIREMENTS FOR ARTICLE III STANDING

"A plaintiff establishes Article III standing by demonstrating (1) an 'injury in fact' that is (2) fairly traceable to the challenged action of the defendant and is (3) likely to be redressed by a favorable decision." *Barrows v. Becerra*, 24 F.4th 116, 127 (2d Cir. 2022) (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560–61 (1992)). "[A]t the pleading stage, 'general factual allegations of injury resulting from the defendant's conduct may suffice'" to satisfy the requirements of standing." *John v. Whole Foods Mkt. Grp., Inc*., 858 F.3d 732, 736 (2d Cir. 2017) (quoting *Lujan*, 504 U.S. at 561). Here, Plaintiffs sufficiently plead each element of standing and so, contrary to GEICO's arguments (MTD at 6-19), Plaintiffs have standing, and this Court has subject matter jurisdiction.

A. GEICO's Use and Disclosure of Plaintiffs' PI Caused Article III Injury-In-Fact.

Plaintiffs seeking redress for intangible injuries, such as invasion of privacy or intrusion upon seclusion, have obtained redress in federal courts for centuries. The Supreme Court explicitly recognized as much in *Spokeo*, noting that intangible injuries have long been "concrete" "injuries in fact" for purposes of Article III. *Spokeo, Inc. v. Robins*, 578 U.S. 330, 340 (2016)*, as revised* (May 24, 2016) ("[W]e have confirmed in many of our previous cases that intangible injuries can nevertheless be concrete.") (citing cases). The *Spokeo* Court also recognized that Article III of the Constitution did not freeze the scope of actionable injuries to those that were actionable in 1776. To the contrary, Congress retains the right to "elevat[e] to the status of legally cognizable injuries concrete, *de facto* injuries that were previously inadequate in law." *Id.* at 341 (quoting *Lujan* 504 U.S. at 578). But Congress's power to create new injuries is not unfettered. Instead, to be actionable in federal court, a statutorily created injury must be analogous, not identical, to an injury

that was actionable at common law. A plaintiff proceeding under a statutory cause of action can therefore establish a cognizable injury by "identif[ying] a close historical or common-law analogue for their asserted injury" for which courts have "traditionally" provided a remedy. *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2204 (2021) (explaining that such analogs "include, for example, reputational harms, *disclosure of private information*, and intrusion upon seclusion") (emphasis added);[2] *see also Mount v. PulsePoint, Inc.*, 684 F. App'x 32, 34 (2d Cir. 2017)*, as amended* (May 3, 2017) (finding Article III standing where a plaintiff pleads "a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts") (internal quotations and citation omitted); *Cooper v. Slice Techs., Inc.*, No. 17-CV-7102 (JPO), 2018 WL 2727888, at *3 (S.D.N.Y. June 6, 2018) (recognizing conduct that "implicates harms similar to those associated with the common law" such as the "tort of intrusion upon seclusion . . . satisfy the requirement of concreteness"). In short, a plaintiff who pleads a statutory injury that is analogous (but not identical) to an injury that was actionable at common law "*has standing even if the precise injury would not, absent the statute, be sufficient for Article III standing purposes*." *Garey v. James S. Farrin, P.C.*, 35 F.4th 917, 921-22 (4th Cir. 2022) (emphasis added) (finding injury in DPPA case).

---

[2] *TransUnion* is wrongly cited by Defendants to suggest privacy harms cannot constitute concrete injury-in-fact (MTD at 11-12), as that decision explicitly affirms *Spokeo*'s holding that "[v]arious intangible harms can [] be concrete . . . for example, . . . *disclosure of private information* . . . ." *Id.* at 2204 (emphasis added). The Supreme Court in *TransUnion* had "no trouble" concluding that class members whose credit reports containing false information were provided to a third party in violation of the Fair Credit Reporting Act ("FCRA") had "suffered a concrete harm that qualifies as an injury in fact." *Id.* at 2208-09. No showing was required to establish standing beyond provision of the credit reports to third parties in violation of the FCRA, not even that anyone had read them. *Id.* The only plaintiffs that lacked Article III standing in *TransUnion* were those whose inaccurate credit reports "mere[ly] exist[ed] . . . in a database" at TransUnion, and indisputably had never been disclosed to a third party. *Id.* at 2209-10. That scenario does not apply here, where GEICO voluntarily transmitted DPPA-protected data through its online quoting platforms directly to malicious third-party actors. CAC ¶¶ 56-61; 69-72.

Congress enacted the DPPA to respond to the concern "that personal information collected by States in the licensing of motor vehicle drivers was being released—even sold—with *resulting loss of privacy for many persons*." *Maracich v. Spears*, 570 U.S. 48, 51–52 (2013) (emphasis added). GEICO violated the DPPA by using and disclosing Plaintiffs' and thousands of putative class members' protected driver's license numbers for an improper purpose. The statutory injury here, which is analogous to an invasion of privacy, which was actionable at common law, therefore, constitutes a concrete injury-in-fact for purposes of Article III, giving Plaintiffs the right to sue for statutory damages in federal court. 18 U.S.C. § 2724(a)-(b); *In re USAA*, 2022 WL 3348527, at *5.

The Southern District of New York, alongside numerous federal circuit and district courts, recognizes that "plaintiffs plausibly allege injury-in-fact in the form of a loss of privacy protected under the DPPA." *Id.* at *4-*5; *see also Garey*, 35 F.4th at 921 (finding that the DPPA, a consumer privacy statute, confers Article III standing because the "alleged harms are closely related to the invasion of privacy, which has long provided a basis for recovery at common law");[3] *Allen v. Vertafore, Inc.*, 4:20-cv-04139, 2021 WL 3148870, at *2 (S.D. Tex. June 14, 2021) *report and recommendation adopted,* No. 4:20-CV-04139, 2021 WL 3144469 (S.D. Tex. July 23, 2021), *aff'd,* 28 F.4th 613 (5th Cir. 2022), *cert. denied sub nom. Allen v. Vertavore, Inc.,* No. 21-

[3] In *Garey*, the defendants obtained car accident reports from North Carolina law enforcement agencies and private data brokers that included names and addresses of drivers involved in car accidents. *Id.* at 919. The defendants then used that information to solicit potential clients. *Id.* The plaintiffs brought suit on behalf of a putative class, alleging violations of the DPPA. *Id.* at 919-20. In concluding that the plaintiffs had Article III standing, the Fourth Circuit found that the alleged harms "are closely related to the invasion of privacy, which has long provided a basis for recovery at common law." *Id.* at 921. As the Fourth Circuit concluded, "[a]t bottom, the DPPA is aimed squarely at 'the right of the plaintiff, in the phrase coined by Judge Cooley, 'to be let alone.'" *Id.* (quoting William L. Prosser, Privacy, 48 Calif. L. Rev.383, 389 (1960) (footnote omitted)) (citing Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890)).

1555, 2022 WL 4652002 (U.S. Oct. 3, 2022) (explaining disclosure of sensitive data in violation of the DPPA is sufficient to establish Article III standing).

As discussed at length in Section II, *infra*, Plaintiffs and class members sufficiently allege a legally cognizable privacy injury resulting from GEICO's improper disclosure of their sensitive personal and driving information to third parties in violation of the DPPA. *E.g.*, CAC ¶ 123 ("As a result of the events detailed herein, *Plaintiffs and Class Members suffered harm and loss of privacy* . . . because of GEICO's Data Disclosure and the fact that their driver's license numbers are now in the hands of criminals") (emphasis added). Because the type of harm caused here—the disclosure of private information—is harm that the DPPA protects against and is a long-recognized basis for tort actions in English and American courts, the injury Plaintiffs suffered as a result of GEICO's violation of the DPPA is an injury "in fact" that is sufficiently "concrete" to confer Article III standing. *TransUnion LLC*, 141 S. Ct. at 2204.

B. Efforts to Mitigate Existing Identity Theft Constitute Injuries-in-Fact

Plaintiffs also allege a separate, independently sufficient basis for Article III standing, namely that they have already experienced fraud as a result of GEICO's Data Disclosure, requiring them to expend significant time and effort to address the misuse of their PI. CAC ¶¶ 11-12, 113, 123, 167, 182. Specifically, Plaintiff Viscardi alleges lost time and money to resolve two fraudulent applications for unemployment benefits, an unauthorized attempt to transfer funds from his bank account, fraudulent charges attempted on his Chase Bank credit card, and fraudulent charges totaling approximately $1,000 on his Bank of America VISA card. *Id*. ¶¶ 17-26. Plaintiff Dorety alleges lost time and money—including the filing of two different police reports—associated with a fraudulent claim for unemployment benefits and a fraudulent checking account opened in her name, which notably incurred fraudulent transactions. *Id*. ¶¶ 31-37. Similarly,

Plaintiff Morgan alleges the loss of time and money to address a fraudulent claim for unemployment benefits which led to the freezing of his credit. *Id*. ¶¶ 42-47.

Courts routinely recognize that allegations of "significant time, effort, and resources" spent "responding to [] already-occurred identity thefts are sufficient to demonstrate a concrete injury for the purpose of Article III standing." *In re USAA*, 2022 WL 3348527, at *5; *Rudolph v. Hudson's Bay Co.*, No. 18-cv-8472-PKC, 2019 WL 2023713, at *6 (S.D.N.Y. May 7, 2019) (finding that loss of time addressing fraudulent charges and identity theft as a result of a data breach is sufficient to meet the "low threshold" for Article III standing); *see Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 692 (7th Cir. 2015) (same).

GEICO's reliance on inapposite case law—most of which are out-of-circuit decisions—does not undermine Plaintiffs' allegations of direct tangible harm suffered as a result of the Data Disclosure. Importantly, all of the cases relied upon by GEICO suffer from a singular, common fault: the plaintiffs failed to allege mitigation efforts for harm that has already occurred and is ongoing. *See* MTD at 8-9.

First, in *Whalen v. Michael Stores, Inc.*, 153 F. Supp. 3d 577, 581 (E.D.N.Y. 2015) the court held that allegations of loss of time and money associated with future misuse of plaintiffs' information as a result of a data breach were "manufactured" and implausible, as the plaintiff had replaced the credit card that was allegedly compromised and did not experience any fraud in a two-year period. Plaintiffs here do not allege expenditure of time and effort merely to prevent possible future harm. They allege mitigation of harm that has already occurred—such as fraudulent insurance and unemployment claims—and is actively occurring. Further distinguishing *Whalen* is the fact that the plaintiff in that case could easily remediate any risk of future harm merely by cancelling her credit card. *Id*. at 580.

Second, *Greenstein v. Noblr Reciprocal Exchange*, No. 21-cv-04537-JSW, 2022 WL 472183, at *5 (N.D. Cal. Feb. 15, 2022) is distinguishable because the plaintiff there did not allege the expenditure of time or effort to resolve or remediate actual fraud, like Plaintiffs have pleaded here.[4]

Finally, in *Baysal v. Midvale Indemnity Company*, the court found that the plaintiffs' lacked standing to recover for the loss of time and expenses to monitor for the abstract and non-imminent possibility of future harm where the complaint failed to allege "actual harm to one of the plaintiffs." No. 21-cv-394-WMC, 2022 WL 1155295, at *2 (W.D. Wis. Apr. 19, 2022). The *Baysal* court acknowledged that having to take action to remediate the "imminency of [] harm" is a sufficient injury where the complaint includes fraud or misuse that has already occurred. *Id.* at *3. The court identified allegations such as "misuse of credit card information or by concrete examples of some plaintiffs suffering a concrete harm from the data breach." *Id*. (pointing to a list of alleged harms that could happen when PI is disclosed); *cf. Park v. Am. Fam. Life Ins. Co.*, No. 22-cv-171-WMC, 2022 WL 2230171, at *2 (W.D. Wis. June 17, 2022) (distinguishing *Baysal* in related breach and holding victims had standing to challenge instant quote disclosure of driver's license numbers).

In contrast to *Whalen*, *Greenstein*, and *Baysal*, Plaintiffs' allegations of actual fraud attempts distinguish the risk of possible access to driver's license numbers from proven access to driver's license numbers. Accordingly, "[b]ecause these alleged losses implicate monetary harm directly caused by the [data disclosure], they are sufficiently concrete to constitute an injury-in-fact." *In re USAA*, 2022 WL 3348527, at *5.

---

[4] The court in *Greenstein* also allowed the Plaintiffs to re-plead their complaint allegations and a second motion to dismiss is currently pending. *See id.* at *8; *see also Greenstein v. Noblr Reciprocal Exchange*, No. 4:21-cv-04537 (N.D. Cal.), ECF Nos. 42-44.

C. "Certainly Impending" Risk of Identity Theft Constitutes an Injury-in-Fact

Plaintiffs also have Article III standing to bring their claims based upon an imminent risk of future harm. As the Supreme Court acknowledged in *Spokeo*, the risk of future harm can satisfy Article III. 578 U.S. at 34. In the recent decision in *McMorris v. Carlos Lopez & Associates*, *LLC*, the Second Circuit held that plaintiffs can establish standing based solely on an increased risk of future identity theft or fraud following an unauthorized disclosure of personal data. 995 F.3d 295, 300-01 (2d Cir. 2021) (citing *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014)).

The data breach in *McMorris* involved the disclosure of a spreadsheet containing the personal information of a company's current and former employees to all current employees within the company. *Id*. at 298. The Second Circuit concluded that the *McMorris* plaintiffs did not establish Article III standing because, in contrast to Plaintiffs here, the plaintiffs "did not allege that the PII in the spreadsheet was ever shared with anyone outside of [the company] or taken or misused by any third parties." *Id*. The Second Circuit identified three non-exhaustive factors for determining whether an increased risk of identity theft following the disclosure of personal information carries a threat of impending harm sufficient to confer Article III standing:

> (1) whether the plaintiffs' data has been exposed as the result of a targeted attempt to obtain that data; (2) whether any portion of the dataset has already been misused, even if the plaintiffs themselves have not yet experienced identity theft or fraud; and (3) whether the type of data that has been exposed is sensitive such that there is a high risk of identity theft or fraud.

Id. at 303. Applying these factors here weighs in favor of finding Plaintiffs have standing.

First, the Data Disclosure was the result of a "targeted attempt to obtain" sensitive driver's license numbers of thousands of individuals as part of an industry-wide scheme to exploit insurance companies' disclosures via their online quoting platform. CAC ¶¶ 9-10, 60-61, 69-75, 93. The cybercriminals had no reason to input Plaintiffs' information in GEICO's website other

than to obtain their driver's license for nefarious purposes. *See In re USAA*, 2022 WL 3348527, at *5; *In re GE/CBPS Data Breach Litig.*, No. 20-cv-2903-KPF, 2021 WL 3406374, at *6 (S.D.N.Y. Aug. 4, 2021) (allegations that "'an unauthorized party' gained access to [. . .] employees' PII" satisfied the first *McMorris* factor); *see also McMorris*, 995 F.3d at 301 ("Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities.") (citing *Remijas*, 794 F.3d at 693); *accord* CAC ¶ 83. GEICO admitted as much in its Notice of Data Breach by warning impacted customers that "[w]e have reason to believe [the disclosed driver's license numbers] could be used to fraudulently apply for unemployment benefits in your name." CAC ¶¶ 17, 30, 41.

Second, the Complaint is replete with examples of Plaintiffs' and class members' driver's license being misused to commit widespread unemployment fraud (*e.g.*, CAC ¶¶ 18-20 (Viscardi); ¶¶ 31-33 (Dorety); ¶¶ 42-43 (Morgan)), financial fraud (*e.g.*, *id*. ¶¶ 21-24 (Viscardi); ¶ 34 (Dorety)), and identity theft (*e.g.*, *id*.). The actual misuse of Plaintiffs' and class members' driver's license numbers is unsurprising in view of the alerts issued by the New York Department of Financial Services to insurance companies—particularly those, like GEICO, that offer instant online insurance quotes—to provide warning that the unauthorized collection of driver's license numbers appears to be part of a growing fraud campaign targeting pandemic and unemployment benefits. *Id*. ¶ 71. These allegations satisfy the prong of misuse of the improperly obtained data. *See In re GE/CBPS Data Breach*, 2021 WL 3406474, at *6; *see also McMorris*, 995 F.3d at 304 (collecting cases in which some part of the exposed dataset was shown to have been compromised).

Third, Plaintiffs allege in detail the sensitivity of driver's license numbers and how that information creates a "high risk of identity theft or fraud" and the value of driver's license numbers to criminals. CAC ¶¶ 53, 62-67, 69, 71-77, 82-95. Driver's license numbers are particularly

sensitive because, among other things, they are "uniquely connected to the ability to file unemployment benefit claims [and to] commit other financial fraud," they are "significantly more valuable than [] credit card information [] because there, victims can cancel or close credit and debit card accounts [but driver's license numbers] can be used to *open* fraudulent bank accounts and credit and debit cards or take out loans, especially student loans [and are] long lasting, and difficult to change," and, unlike credit or debit card numbers, driver's license numbers cannot be quickly frozen, reissued, or replaced. *See id*. ¶¶ 82-95. GEICO's suggestion that driver's license numbers are not sensitive is unavailing. *See* MTD at 11.[5] Not only does GEICO contradict the admissions it made in its own Notice of Data Breach, but the insurance industry consistently recognizes driver's license numbers as sensitive information that must be protected from unauthorized exfiltration. CAC ¶¶ 10, 17, 30, 41 (GEICO's Notice warning affected persons that the information extracted from their platform "could be used to fraudulently apply for unemployment benefits"); *see also id*. ¶¶ 82-95. Thus, Plaintiffs "plausibly allege their driver's license numbers are sufficiently sensitive such that there is a high risk of identity theft or fraud upon their disclosure." *In re USAA*, 2022 WL 3348527, at *6 (internal quotations omitted); *see also Park*, 2022 WL 2230171, at *2 (finding that the plaintiff alleged an "objectively reasonable likelihood that an injury will occur" as a result of cybercriminals' theft of driver's license numbers

[5] While it does not impact Plaintiffs' standing in this case on the multiple bases outlined above, *In re USAA* misinterprets one aspect of *TransUnion*. The *In re USAA* Court takes the quote "the mere risk of future harm, standing alone, cannot qualify as a concrete harm—at least unless the exposure to the risk of future harm itself causes a separate concrete harm" (*TransUnion*, 141 S.Ct. at 2210-11) to suggest that "*TransUnion* appears to have abrogated" the ruling in *McMorris* that "a sufficiently imminent risk of identity theft, standing alone, could constitute injury-in-fact." 2022 WL 3348527, at *4 and n.2. In fact, the "mere risk" to which *TransUnion* refers in this quote is to the "mere presence of an inaccuracy in an internal credit file, if it is not disclosed to a third party." 141 S. Ct. at 2210. As *TransUnion* had already explained, once the offending information was "published to a third party," it ceased to be a "mere risk" and constituted the type of "substantial risk" that supports Article III standing, consistent with *McMorris*.

automatically disclosed in online quotes).[6]

The Complaint provides ample allegations to support each *McMorris* factor, and Plaintiffs have plausibly alleged injury-in-fact based on a substantial risk of identity theft.

D. Plaintiffs' Injuries Are Fairly Traceable to the Data Disclosure and Likely to Be Redressed by a Favorable Judicial Decision

Plaintiffs adequately plead that their injuries are "fairly traceable" to the Data Disclosure. Traceability "is a standard lower than that of proximate causation." *Carter v. HealthPort Techs., LLC*, 822 F.3d 47, 55 (2d Cir. 2016). Plaintiffs have alleged that shortly after GEICO disclosed their driver's license numbers, they suffered the very types of fraudulent activities that are typically associated with the theft of driver's license numbers, including fraudulent unemployment claims and fraudulent accounts opened in their names. CAC ¶¶ 18-22, 31-34, 42-43. Nothing more is necessary. *See*, *e.g.*, *In re USAA*, 2022 WL 3348527, at *4 n.3.

Plaintiffs' injuries are also "likely to be redressed by a favorable judicial decision." *Spokeo*, 578 U.S. at 338. Plaintiffs plausibly allege their entitlement to statutory damages from the disclosure of their driver's license information in violation of the DPPA. Statutory or nominal damages constitute sufficient redress for Article III. *Uzuegbunam v. Preczewski*, 141 S. Ct. 792, 802 (2021) ("[A] request for nominal damages satisfies the redressability element of standing where a plaintiff's claim is based on a completed violation of a legal right."); *See* Section II, *infra*. In addition, Plaintiffs have alleged actual damages in the forms of, *inter alia*, lost time and effort

[6] It is immaterial that some of the compromised information at issue here "is publicly available even in the absence of any data breach," because the exposure of affected persons' driver's license numbers "provides hackers the means to commit fraud or identity theft by way of a social engineering attack." *See In re GE/CBPS Data Breach*, 2021 WL 3406374 at *7; *see also Bass v. Facebook, Inc*., 394 F. Supp. 3d 1024, 1033-35 (N.D. Cal. 2019) (finding that "information taken . . . need not be sensitive to weaponize hackers in their quest to commit further fraud or identity theft," and even an individual's email address, mailing address and employment information can "provide further ammo" to "nefarious actors").

remediating and mitigating fraud they have already experienced and imminent future harm. Those injuries are legally cognizable. *See McFarlane v. Altice USA, Inc.*, 524 F. Supp. 3d 264, 273 (S.D.N.Y. 2021) ("[I]f Plaintiffs succeed on the merits of their claims, the Court can redress their injuries by awarding damages for the 'reasonabl[e]' costs of 'mitigat[ing] or avoid[ing] future identity theft, among other things.") (citation omitted).

Plaintiffs' claims for declaratory judgment and injunctive relief are alternative means of redress. In addition to harm already suffered as a result of GEICO's Data Disclosure, Plaintiffs and class members will continue to be injured because GEICO's subsequent remedial measures, such as "a year of credit monitoring" are "woefully inadequate," and GEICO continues to implement inadequate security measures for the future protection and security of sensitive PI. CAC ¶¶ 101-02, 202-06. "Because plaintiffs 'plausibly allege[] the continued inadequacy of [the insurer's] security measures' they 'plausibly allege that they face a substantial risk of future harm if [the insurer's] security shortcomings are not redressed, making this dispute sufficiently real and immediate with respect to the parties' 'legal relations, which are adverse.'" *In re USAA*, 2022 WL 3348527, at *11 (citation omitted). Thus, Plaintiffs' claims are likely to be redressed by damages, declaratory judgment, and injunctive relief, fulfilling the third prong of Article III standing.

II. PLAINTIFFS ADEQUATELY PLEAD THAT GEICO VIOLATED THE DPPA

A violation of the DPPA exists where: (1) a defendant knowingly obtained, disclosed, or used personal information; (2) from a motor vehicle record; (3) for a purpose not permitted." *Mallak v. Aitkin Cnty.*, 9 F. Supp. 3d 1046, 1055 (D. Minn. 2014); *see* 18 U.S.C. § 2724(a). These protections were born out of Congress' concern "that personal information collected by States in the licensing of motor vehicle drivers was being released—even sold—with resulting loss of privacy for many persons." *Maracich*, 570 U.S. at 52. The DPPA holds that "it is 'unlawful for

any person knowingly to obtain or disclose personal information, from a motor vehicle record, for any use not permitted under section 2721(b).'" *Cowan v. Ernest Codelia, P.C.*, No. 98-cv-5548-JGK, 2001 WL 856606, at *8 (S.D.N.Y. July 30, 2001) (quoting 18 U.S.C. § 2724(a)). "The default rule is one of non-disclosure." *In re USAA*, 2022 WL 3348527, at *6.

The DPPA also provides a second layer of protection to drivers' privacy by regulating "the resale and redisclosure of drivers' personal information by private persons who have obtained that information from a state DMV." *Id*. In *In re USAA*, the Southern District of New York recognized that the Second Circuit imposes "a duty of reasonable care" upon authorized recipients of PI who redisclose such information to subsequent downstream users. *Id*. (quoting *Gordon v. Softech Int'l*, 726 F.3d 42, 56-57 (2d Cir. 2013)).

Plaintiffs' well-pleaded allegations satisfy each element under the DPPA by alleging that that GEICO knowingly obtained, used, and disclosed Plaintiffs' sensitive PI to third parties, including their driver's license information, for a purpose not permitted under the Act and without the required due care.

A. GEICO Knowingly Disclosed Plaintiffs' Protected Driver's License Numbers to Unauthorized Third Parties

Plaintiffs' allegations support the conclusion that GEICO's decision to automatically populate its insurance quote forms with Plaintiffs' driver's license numbers constitutes a knowing disclosure under the DPPA. Courts consistently find that a "'knowing disclosure' is merely a disclosure made voluntarily. *See Senne v. Vill. of Palatine, Ill.*, 695 F.3d 597, 603 (7th Cir. 2012) ("Voluntary action, not knowledge of illegality or potential consequences" is sufficient under the DPPA); *Enslin v. The Coca-Cola Company*, 136 F.Supp.3d 654, 670 (E.D. Pa. 2015) ("A knowing disclosure of PDI requires the defendant take some voluntary action to disclose the information.") (internal quotations and citation omitted). "Knowing" does not mean "knowledge of illegality or

potential consequences.'" *In re USAA*, 2022 WL 3348527, at *7 (quoting *Senne*, 695 F.3d at 603 (7th Cir. 2012) (finding that the placement of a printed driving citation on a driver's windshield for public view is "th[e] sort of publication [that] is certainly forbidden by the statute.")); *see also Pichler v. UNITE*, 542 F.3d 380, 396 (3d Cir. 2008) (rejecting the argument that "civil liability requires a defendant knowingly obtain or disclose personal information for a use the defendant knows is impermissible"). Accordingly, "knowing" is a low bar under the DPPA.

Consistent with the requirements of the DPPA, Plaintiffs allege that "GEICO effectively posted consumers' driver's license numbers on the internet's 'windshield,' for all digital passer-by" to see. CAC ¶¶ 8, 57, 58. GEICO previously had a practice of offering online insurance quotes without an auto-population feature, which required a consumer to manually enter all personal information. *Id.* ¶ 143. However, in a decision that prioritized its sales and profits over data privacy, GEICO "chose to add a feature to its existing online sales platform where an individual's driver's license number would auto-populate for anyone that would enter a bare minimum of publicly available information about that individual." *Id.* ¶¶ 6, 59, 78. Plaintiffs allege that "GEICO intended to make the displayed information . . . easily accessible to anyone who entered basic information into its system." *Id.* ¶ 8. The voluntary and knowing disclosure alleged here—placing Plaintiff's sensitive, PI on GEICO's website for immediate and unhindered public view—is sufficient to come within the activity regulated by the DPPA. *Id.* ¶ 56 ("GEICO has an online sales system available to all persons capable of accessing it via the internet). This is so "regardless of whether another person viewed the information or whether [GEICO] intended it to be viewed on by [the insurance claimant] himself." *Senne*, 695 F.3d at 603.

GEICO makes an unavailing attempt to undermine Plaintiffs' claim by relying on inapposite cases that involve breaches and hacking, and the resultant theft of PI from otherwise

secured servers without any affirmative act by the defendant. *See* MTD at 20-21 (citing *Allen*, 2021 WL 3148870, at *9 (involving an unauthorized data breach of external servers)); *Enslin*, 136 F.Supp.3d at 670 (involving the theft of 55 laptops containing PI of employees); *McDonough v. Anoka County*, 799 F.3d 931, 957 (8th Cir. 2015) (involving an agency employee using a password to improperly access databases containing PI); *Gulsvig v. Mille Lacs County*, No. CIV. 13-1309 JRT/LIB, 2014 WL 1285785, at *6 (D. Minn. Mar. 31, 2014) (involving an agency employee improperly accessing information stored on a state database)). Notably, in each of these cases, the respective court emphasized the complete absence of any factual allegation that the defendant acted voluntarily to facilitate the alleged disclosure. *See*, *e.g.*, *Allen*, 2021 WL 3148870 at *3 ("To be clear, the facts alleged in the Complaint describe Vertafore as having stored the data on servers under Vertafore's control, meaning the data was never actually knowingly disclosed to anyone outside of Vertafore."); *Enslin*, 136 F. Supp. 3d at 671 ("Plaintiff does not describe any allegedly improper disclosure of Plaintiff's PDI by one Coke Defendant to another; rather, Plaintiff speaks in general terms about the 'Coke Defendants' retention of his PDI.").

Plaintiffs' DPPA claim does not suffer from the same pitfall that precluded a finding of a "knowing disclosure" in these cases. Rather, Plaintiffs' allegations make clear that GEICO acted voluntarily to publish Plaintiffs' driver's license numbers to GEICO's publicly available website, allowing for immediate, unhindered access and consumption by unknown third parties. *See* CAC ¶¶ 8, 58, 61. As the court in *Enslin* recognized, a theft of "unsecured information on privately held laptops [or internal servers] is different from placing the information on the windshield of [a] vehicle in plain view on a public way," and Plaintiffs' allegations against GEICO here are more akin to the latter. *Id*. at 671.

This Court's sister district court reached the same conclusion in *In re USAA* where

Plaintiffs alleged that USAA "designed its website to ensure users could apply for its insurance policies as seamlessly as possible. 2022 WL 3348527, at *1. Specifically, "an individual seeking a quote for any of USAA's insurance policies could do so by first creating a USAA account, which requires providing 'minimal information,'" and "once the account is made, the USAA member would then receive an online quote form pre-filled with personally identifiable information ('PII') regarding the member drawn from the relevant state's department of motor vehicles ('DMV'), including the member's driver's license number." *Id*. In denying the motion to dismiss the DPPA claim, Judge Vincent L. Briccetti concluded that "USAA's voluntary decision to automatically pre-fill its quote forms with driver's license numbers constitutes a knowing disclosure of personal information." *Id.* at *7 (citing 18 U.S.C. § 2724(a)). Judge Briccetti further identified that "USAA reasonably should have known its pre-filling of driver's license numbers would disclose that protected information directly to cybercriminals for impermissible purposes." *In re USAA,* 2022 WL 3348527, at *7.

In re USAA is directly on point and controls the outcome here where there are analogous factual circumstances. Plaintiffs here make similar allegations as the *In re USAA* plaintiffs, and adequately allege that GEICO's decision to pre-fill driver's license numbers on its quote forms knowingly disclosed PI in contravention of the DPPA. Knowing disclosure is adequately pleaded.

B. Plaintiffs Allege That GEICO Obtained PI from a Motor Vehicle Record

Plaintiffs also sufficiently plead that GEICO obtained Plaintiffs' PI from a motor vehicle record. Under the DPPA, "state DMVs, individuals, organizations, and entities may not disclose 'personal information' *drawn from* motor vehicle records unless permitted by statute." *Gordon*, 726 F.3d at 48 (emphasis added). The DPPA's reach extends to "the resale and redisclosure of drivers' personal information by private persons who have obtained that information from a state

DMV." *Reno v. Condon*, 528 U.S. 141, 146 (2000). Accordingly, a private actor who re-discloses information derived from a state motor vehicle record can be held liable for misuse of the information by downstream recipients. *See Gordon*, 726 F.3d at 49.

Plaintiffs' allegations are consistent with the language of the DPPA and explicitly state that GEICO sourced Plaintiffs' driver's license numbers from a motor vehicle record and subsequently disclosed that information without a permissible purpose. *E.g.,* CAC ¶¶ 138-39, 156. Plaintiffs allege that GEICO "collects and stores vast amounts of personal information and sensitive data" to use in their regular course of business, thus qualifying GEICO as an "authorized recipient" under the DPPA. *Id.* ¶ 53. GEICO's online sales system, available to all persons with access to the internet, uses basic information entered by a website visitor, combines it with additional information that GEICO obtained "*from motor vehicle records directly from state agencies*, or through resellers or third party prefill services," and then automatically displays the additional information to the visitor as part of the quote process. *Id.* ¶¶ 56-58, 156 (emphasis added). Specifically, GEICO's automatic quoting feature has potential customers input their name, date of birth, and address and uses that information to populate the insurance quote with driver's license information obtained from state agencies, resellers, or third-party prefill services. *Id*. Importantly, GEICO's access to driver's license information extends to people who never applied for insurance with GEICO or were even aware of GEICO's existence. *Id*. ¶ 60. Once GEICO displays Plaintiffs' sensitive information for public view, GEICO assumes the identity of a re-discloser of PI obtained from a motor vehicle record under the DPPA.

In *In re USAA*, the Southern District of New York found that parallel allegations were sufficient to "plausibly allege [plaintiffs'] driver's license numbers were 'obtained from the relevant state DMVs,' and thus were disclosed 'from a motor vehicle record.'" 2022 WL 3348527

at *7. There, USAA auto-populated responses to requests for insurance quotes with certain personal information, including driver's license numbers. *Id*. at *1. Similar to GEICO's quoting process, individuals seeking an insurance quote through USAA had to provide only minimal information; any additional information needed to process the request was obtained from the state's DMV or other third-party data aggregators. *Id*. Ultimately, cybercriminals recognized the same weakness in USAA's automated quotation process as they did in GEICO's and used the plaintiffs' personal information to create fraudulent USAA accounts and steal plaintiffs' automatically populated driver's license numbers. *Id*. at *2. Based on those allegations, which notably mirror Plaintiffs' allegations here, the court found a viable DPPA claim was pleaded against USAA. *Id*. at *7.

Just like in *In re USAA*, it is immaterial that third-party bad actors were the ultimate end-users of the disclosed information, because GEICO is liable for the subsequent misuse of information derived from state motor vehicle records that it disclosed to downstream users as an authorized recipient.[7] *Id*.; *see also Gordon*, 726 F.3d at 53 (rejecting defendant's motion for summary judgment because "if [the downstream user] was not eligible to claim th[e] exception, [the defendant's] disclosure would have been for a use not permitted by section 2721(b)" in violation of the DPPA). Like the plaintiffs in *In re USAA*, Plaintiffs adequately have pleaded that

[7] GEICO's argument that Plaintiffs make only conclusory allegations as to the source of the PI at issue is unavailing. Plaintiffs allege that GEICO obtained Plaintiffs' PI, including driver's license numbers, from state agencies or a third-party pre-fill service. CAC ¶¶ 57-58, 139, 156. GEICO, as the second largest auto insurance company in the United States, gains access to consumer driving information even without a consumer manually inputting their information into an insurance quote form on GEICO's website. *Id.* ¶¶ 4, 48. This reality is bolstered by the fact that third-party cybercriminals were able to submit insurance quote forms for people who never applied for insurance with Defendant or were even aware of GEICO's existence. *Id.* ¶ 60. Plaintiffs' allegations are a far cry from simply stating that their PI "can be linked back or derived from" a motor vehicle record. *See* MTD at 24 (citing *Garey*, 35 F.4th at 927 (involving a law firm's purchase of car accident reports compiled by data brokers for legal solicitation purposes)).

GEICO obtained Plaintiffs' protected driver's license numbers from a state motor vehicle record.

C. GEICO Did Not Disclose Plaintiffs' Driver's License Numbers to Unauthorized Third Parties for a Proper Purpose Under the DPPA

The mere fact that GEICO is a provider of insurance does not automatically qualify the disclosures at issue for protection under § 2721(b)(6), a conclusion that Plaintiffs' allegations support. The DPPA provides that, unless one of its enumerated exceptions applies, a covered entity "shall not knowingly disclose or otherwise make available" protected personal information. *See* 18 U.S.C. §§ 2721(a)(1)-(2). The Supreme Court directs courts to narrowly interpret the enumerated exceptions to the DPPA's general prohibition against disclosure of PI "in order to preserve the primary operation" of the Act. *Maracich*, 570 U.S. at 60 (examining the DPPA's litigation exception and noting that "unless commanded by the text . . . these exceptions ought not operate to the farthest reach of their linguistic possibilities if that result would contravene the statutory design."). Consistent with this direction, several federal circuit courts have found that "an authorized recipient, faced with a general prohibition against further disclosure, can disclose the information only in a manner that does not exceed the scope of the authorized statutory exception." *Senne*, 695 F.3d at 606; *see also Pichler*, 542 F.3d at 395. Accordingly, "the actual information disclosed . . . must be information that is used for the identified purpose. When a particular piece of disclosed information is not used to effectuate that purpose in any way, the exception provides no protection for the disclosing party." *Senne*, 695 F.3d at 606.

Directly at issue here is the insurance exception, which allows for disclosure of PI "for use by any insurer . . . in connection with claims investigation activities, antifraud activities, rating or underwriting." 18 U.S.C. § 2721(b)(6). Plaintiffs' allegations support the conclusion that although GEICO may have been an authorized recipient of Plaintiffs' PI for some purposes, it also obtained, used, and disclosed Plaintiffs' driver's license numbers for an impermissible profit-seeking

purpose that does not qualify for protection under § 2721(b)(6).[8] Specifically, Plaintiffs allege that GEICO collects and stores a vast amount of sensitive PI as part of its regular business practice of offering automobile insurance, which includes Plaintiffs' driver's license numbers. CAC ¶¶ 4, 52, 53. GEICO may obtain, collect, and use this information—within GEICO's secure internal servers—at least in part for use in the insurance claims process. *Id*. But, while GEICO may collect, store, and otherwise use Plaintiffs' protected driver's license numbers for a purpose consistent with § 2721(b)(6), Plaintiff alleges that GEICO also obtained used and disclosed their information for impermissible purposes, namely for purely commercial reasons unrelated to processing, rating, or underwriting insurance claims. CAC ¶¶ 5-8, 13, 54-55. The fact that GEICO may have had some permissible uses for obtaining, using and disclosing this information does not render all of its purposes for obtaining, using and disclosing the information permissible. Indeed, GEICO's own historical practices demonstrate that GEICO historically did not use this information in this way. GEICO had a prior practice of offering online insurance quotes to applicants without the incorporation of an auto-population feature. *Id.* ¶¶ 7-8, 143. The disclosure of driver's license numbers to the applicant is plainly not necessary to process an insurance quote; the auto-population feature was implemented to reduce the time it takes for customers to obtain a quote and to eliminate the prospect of people failing to complete the quotation process because they did not wish to provide their drivers' license numbers, all to increase sales volume and revenue for GEICO. *Id.* ¶¶ 7, 8, 55, 143. GEICO divulged this sensitive information despite industry-wide knowledge that

[8] Notably, the Southern District did not address § 2721(b)(6) in allowing a DPPA claim against the insurance provider defendant in *In re USAA* to proceed, thus reinforcing the conclusion that GEICO's substantially similar conduct here is outside the purview of the exception. *See generally In re USAA,* 2022 WL 3348527, at *7 (rejecting a motion to dismiss the plaintiffs' DPPA claim without analyzing the defendant's conduct under the insurance exception). If anything, GEICO's claims are in the nature of an affirmative defense that is not appropriate for resolution on a motion to dismiss.

insurers' instant online auto quoting features are a primary entry point for cybercriminals to access consumers' personal information, a phenomenon the New York State Department of Financial Services alerted entities to on February 16, 2021. *Id.* ¶¶ 71-73.[9]

It is not enough that GEICO is an authorized recipient of Plaintiffs' PI under the insurance exception of § 2721(b)(6) to avoid liability. GEICO conflates the fact that some of its reasons for obtaining and using the protected driver's license information may have been permissible with it having carte blanche to obtain, use, and disclose the information for any reason whatsoever. That is not how the DPPA works. The DPPA "contains no language that would excuse an impermissible [disclosure] merely because it was executed in conjunction with a permissible purpose." *Pichler*, 542 F.3d at 395 ("[I]f [defendant] had three purposes for 'obtain[ing], disclos[ing] or us[ing] [plaintiffs'] personal information' and two of those were 'permissible uses' but the third was not, UNITE would still be liable for the third purpose.") (citation omitted). Defendants may have a proper purpose for obtaining and storing the data apart from their impermissible disclosure of the data. Plaintiffs' allegations are clear that in addition to having a permissible purpose for obtaining and using the data, GEICO also had impermissible purposes. Its use of the data to build its website and its redisclosure of that data was done for business purposes to gain a competitive advantage over other insurance providers in the industry—it was neither necessary nor relevant to the underwriting or rating of an insurance quote. With the DPPA's chief aim of privacy protection in mind, the insurance exception of § 2721(b)(6) cannot be read so broadly as to sweep GEICO's self-motivated commercial conduct into its protection. Plaintiffs plausibly plead that GEICO's

[9] Particularly relevant here, GEICO's auto-populate feature continued during the COVID-19 pandemic up until at least March 1, 2021. CAC ¶¶ 74, 144. During this period, GEICO was aware that the insurance industry was experiencing an increased interest in driver's license numbers for the purpose of submitting fraudulent unemployment claims. *Id.* ¶¶ 74-77.

knowing disclosure of their PI exceeded the scope of § 2721(b)(6) and subjects GEICO to liability under the DPPA.

In addition, Plaintiffs are not required to plead a negative. Building a website that uses PI and making that PI available to the public via the internet is an impermissible use and disclosure under the DPPA. *See*, *e.g.*, *Welch v. Theodorides-Bustle*, 677 F. Supp. 2d 1283, 1286-87 (N.D. Fla. 2010) (upholding DPPA claim where the defendants did not deny that plaintiff's personal information was "made available on the internet" where "an internet user can access the information for any or no reason—or on a whim" and concluding that "alleging specifically that there was a disclosure, and alleging generally that there was no proper purpose for the disclosure, is enough"). GEICO does not deny that Plaintiffs' driver's license was "made available on the internet," which is sufficient at the pleadings stage.

Finally, GEICO does not explain how either the auto populate feature on its website or the public disclosure of motor vehicle information to any person with limited information serves a permissible purpose under the DPPA. It is not enough to say that the information was "used for the purpose of facilitating customer access to insurance." Even if that purpose did fall into 18 U.S.C. § 2721(b)(6) or one of the other 13 exceptions (it does not), even for a permissible purpose the DPPA does not provide for unlimited disclosure. As the Seventh Circuit has observed: "The DPPA was enacted as a public safety measure, designed to prevent stalkers and criminals from utilizing motor vehicle records to acquire information about their victims." *Dahlstrom v. Sun-Times Media, LLC*, 777 F.3d 937, 944 (7th Cir. 2015). The law addressed the problem that "[p]rior to the law's enactment, anyone could contact the department of motor vehicles in most states" and obtain a driver's personal information simply by providing a small bit of data, such as a license plate number. *Id.* "At congressional hearings . . ., numerous witnesses testified about the risks

posed by unfettered public access to motor vehicle records." *Id.* In the guise of offering online insurance quotes conveniently and boosting its own online sales numbers, GEICO has re-created the problem the DPPA was enacted to address: unfettered access to protected motor vehicle records by any member of the public with a small bit of their victim's data and an internet connection. This exceeds the permissible scope of the insurance underwriting exception. *See Senne*, 695 F.3d at 604. Otherwise, for example, an insurer or insurance support organization could openly disseminate and publish driver's license numbers on a public forum—as long as it could be used to facilitate customer access to insurance. This is clearly disallowed under the statute (and remarkably close to GEICO's behavior here).

D. GEICO Did Not Use Reasonable Care in Disclosing PI to Third Parties

Plaintiffs adequately allege that GEICO violated a duty of reasonable care imposed by the DPPA by failing to ensure that protected personal information would not be disclosed for an impermissible use. "In light of the clear congressional intent to safeguard the privacy and safety of drivers," the Second Circuit imposes liability on a reseller or re-discloser of PI "when it fails to use reasonable care to ensure that personal information is being obtained for a permissible purpose." *Gordon,* 726 F.3d at 55-56. Specifically, the Second Circuit recognized that "[i]f resellers may not disclose personal information except as permitted by the DPPA, they must be obliged to make *some inquiry* before concluding that disclosure is permitted." *Id*. at *54 (emphasis added). The Second Circuit rejected the notion that "this obligation could be met simply by accepting an end user's mere 'say-so' in the presence of red flags suggesting the requested information was being sought for an improper purpose." *Id*. The Southern District in *In re USAA* found that the duty of reasonable care articulated by the Second Circuit "applies with equal force" to a re-discloser like GEICO. 2022 WL 3348527, at *7.

GEICO's lack of safeguards to determine the true identity of an end-user before disclosing sensitive PI does not pass muster under the applicable the standard of care. GEICO's auto-population feature disclosed sensitive driver's license numbers to anyone who entered basic information into its system—information that is publicly available and easily accessible, such as a person's name, birth date and address—without any security protocols to ensure that website visitors entered and accessed information only about themselves. CAC ¶¶ 8, 58-61, 78. GEICO knew that the auto-populate feature was active on GEICO's website from the beginning of the COVID-19 pandemic until March 1, 2021, a sensitive period where the insurance industry was wrought with false claims made possible by access to sensitive personal information such as driver's license numbers. *Id.* ¶¶ 72-77, 109-111.[10] Equipped with this knowledge, GEICO ignored red flags suggesting that the inquiries to its website were for an improper use and failed to implement basic safeguards to protect Plaintiffs' information. *Id.* ¶¶ 78, 109, 143. Under similar circumstances, the *In re USAA* Court found that the defendant "reasonably should have known its pre-filling of driver's license numbers would disclose that protected information directly to cybercriminals for impermissible purposes." 2022 WL 3348527, at *7; *see also Gordon*, 726 F.3d at 58 (finding that the defendant's failure to "check[] the accuracy of the purported [claimant's] identity" or "inquire as to the [claimant's] eligibility to invoke the insurance exception" violated the duty of reasonable care under the DPPA).

At this stage, Plaintiffs' allegations sufficiently plead GEICO's disclosure of Plaintiffs' PI to third parties for an improper profit-seeking purpose, as well as GEICO's failure to use

[10] GEICO acknowledged that the use and disclosure of Plaintiffs' sensitive personal information creates a substantial risk of identity theft and fraud and encouraged Plaintiffs to be vigilant "if you receive any mailings from your state's unemployment agency/department." CAC ¶ 80 (quoting GEICO's Notice of Data Breach).

reasonable care in responding to requests for Plaintiffs' sensitive personal information. The motion to dismiss the DPPA claim should be denied.

III. PLAINTIFFS STATE A CLAIM FOR NEGLIGENCE

A claim for negligence under New York law requires a plaintiff to plead: "(1) the existence of a duty on defendant's part as to plaintiff; (2) a breach of this duty; and (3) injury to the plaintiff as a result thereof." *Sackin v. TransPerfect Global, Inc.*, 278 F. Supp. 3d 739, 747 (S.D.N.Y. 2017). Defendant's arguments for dismissal of the negligence claim are threefold: Plaintiffs' fail to allege a duty, proximate causation, and damages. These arguments fail.

A. GEICO Breached a Duty of Care Owed to Plaintiffs

A defendant who collects and retains sensitive information like driver's license numbers on its servers has a common law duty to exercise reasonable care to protect that information. *See In re USAA*, 2022 WL 3348527, at *8. Specifically, the Southern District of New York found that:

> [D]istrict courts applying New York law have found that a duty of care existed when the custodian was 'in the best position to protect information on its own servers from data breach,' 'understood the importance of data security to its business, knew it was the target of cyber-attacks, and touted its data security to current and potential customers . . . .

Id.; *see, e.g.*, *Toretto v. Donnelley Fin. Sols., Inc.*, No. 1:20-cv-2667-GHW, 2022 WL 348412, at *12 (S.D.N.Y. Feb. 4, 2022) (proxy service provider that received investors' PII owed a duty of care to protect such information, *despite lacking a direct relationship* with investors) (emphasis added).

Plaintiffs allege that GEICO owed a duty to Plaintiffs and class members to exercise reasonable care in "obtaining, securing, safeguarding, storing, and protecting . . . PI from being compromised, lost, stolen, and accessed by unauthorized persons" consistent with industry standards. CAC ¶¶ 152-154. GEICO further assumed the duty to exercise reasonable care to protect

sensitive personal and driving information as a result of its own statements touting Geico.com's "[p]hysical safeguards, procedural controls and data access controls [that] protect your data from unauthorized access," which GEICO "continually monitors . . . to prevent unauthorized attempts at intrusion." *Id*. ¶ 155. Federal courts find similar allegations sufficient to plausibly allege a duty of care. *See, e.g.*, *In re USAA*, 2022 WL 3348527, at *8 ("[F]ixing a duty of care under these circumstances best realizes the expectations of the parties without imposing unlimited liability."); *In re GE/CBPS Data Breach*, 2021 WL 3406374, at *8 (finding a "special relationship [] existed between GE and its employees" who are required to "submit non-public, sensitive personal and financial information"); *In re Rutter's Inc. Data Sec. Breach Litig.*, 511 F. Supp. 3d 514, 529-30 (M.D. Pa. 2021) ("Defendant's affirmative act of retaining [personal information] which created a risk of foreseeable harm from unscrupulous third parties is enough to recognize a legal duty here."); *In re Equifax, Inc., Customer Data Security Litig*., 362 F. Supp. 3d 1295, 1326 (N.D. Ga. 2019) ("*In re Equifax*") ; *McKenzie v. Allconnect, Inc.*, 369 F. Supp. 3d 810, 817-818 (E.D. Ky. 2019) ("[Defendant] did have a duty to prevent foreseeable harm to [plaintiffs] and, as part of that duty, had a duty to safeguard the sensitive personal information of [plaintiffs] from unauthorized release or theft.").

GEICO had a common law duty to implement reasonably security measures to protect the sensitive PI it voluntarily collected from state DMV records from being compromised, disclosed, or misused by unauthorized persons. CAC ¶¶ 152-54. Indeed, GEICO's duty is reinforced by the protections afforded to information obtained from a motor vehicle, such as driver's license numbers under the DPPA. *Id*. ¶ 2. GEICO knew that it collected and used sensitive PI as a consequence of its normal business practices. *Id*. ¶¶ 53, 68, 78. It was also aware that insurance companies were the target of a systemic campaign of cybercriminals, given the New York State

Department of Finance's multiple warnings that bad actors were exploiting cybersecurity flaws on similar websites that display prefilled information to generate an insurance quote. *Id*. ¶¶ 71, 93. Equipped with this knowledge, GEICO was in the best position to safeguard the information it had gathered in its custody and, thus, may be expected to "bear the burden of doing so." *In re GE/CBPS Data Breach*, 2021 WL 3406374, at *8. However, GEICO breached this duty by knowingly using federally protected driver's license information to auto-populate insurance quotes on its publicly available website, allowing cybercriminals immediate and unfettered access to the sensitive data at a time when unemployment and pandemic benefit fraud was rampant. CAC ¶¶ 6-8, 77-78, 111; *see also In re USAA*, 2022 WL 3348527, at *8.

B. GEICO's Breach Proximately Caused Plaintiffs' Legally Cognizable Injuries

GEICO's arguments with respect to proximate causation and damages simply restate their arguments with respect to traceability and redressability, which have been addressed in Section I.D, *supra*. GEICO's own communications with Plaintiffs and class members in the Notice of Data Breach make clear that the sensitive personal and driving information that GEICO disclosed to bad actors "could be used" to commit fraud. CAC ¶¶ 10; 79-81. Plaintiffs have alleged that the specific information disclosed by GEICO is particularly valuable to fraudsters, especially during the COVID-19 pandemic, and that its disclosure facilitated fraud. *Id.* ¶¶ 74, 82-95. As a direct and proximate result of the aforementioned misconduct, Plaintiffs plead entitlement to eight distinct categories of damages, each of which supports the negligence claim. *Id*. ¶ 167. GEICO asks the Court to disregard these well-pleaded allegations but, at this stage, the Court is required to take these allegations as true.

GEICO's attempt to point to other similar disclosures in the insurance industry to defeat causation (MTD at 27) is a fact-intensive argument that is routinely rejected at the pleading stage

in data disclosure cases. *In re Equifax*, 362 F. Supp. 3d at 1318 is directly on point. There, the defendants argued that the plaintiffs failed to prove that their injuries resulted from the specific data breach at issue, as opposed to "some other data breach or fraudulent conduct." *Id.* The district court "[found] this argument unpersuasive," and held that the "Plaintiffs need not explicitly state that other breaches did *not* cause these alleged injuries, since their allegations that this Data Breach *did* cause their injuries implies such an allegation." *Id*. (emphasis in original). The district court also noted that "allowing the Defendants 'to rely on other data breaches to defeat a causal connection would "create a perverse incentive for companies: so long as enough data breaches take place, individual companies will never be found liable,"'" and the *Equifax* court "decline[d] to create such a perverse incentive." *Id*. This court should follow suit and reject GEICO's fact-based causation argument.

GEICO's motion to dismiss Plaintiffs' negligence claim must be denied. *See, e.g., Toretto*, 2022 WL 348412, at *13; *In re GE/CBPS*, 2021 WL 3406374, at *9; *In re Cap. One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 405 (E.D. Va. 2020) ("*In re Cap. One*").

IV. PLAINTIFFS STATE A CLAIM FOR NEGLIGENCE PER SE

It is well-established under New York law that the "violation of a statute may constitute negligence per se or it may give rise to absolute liability." *Van Gaasbeck v. Webatuck Cent. Sch. Dist. No. 1*, 21 N.Y.2d 239, 243 (1967) (internal citation omitted); *see also Elliott v. City of New York*, 95 N.Y.2d 730, 734 (2001) (same). A statute can establish a standard of care relevant to a negligence per se action even when the statute does not expressly provide for a private right of action. *Stone v. City of New York*, No. 05-cv-2736-SLT, 2009 WL 10705814, at *10 (E.D.N.Y. Dec. 30, 2009); *accord Coastline Terminals of Connecticut, Inc. v. USX Corp.*, 156 F. Supp. 2d 203, 210 (D. Conn. 2001) ("The statutory basis for a negligence *per se* claim need not provide for

a private right of action."). A defendant is liable for negligence per se if the plaintiff establishes: "(1) that he or she is among the class of people for whose particular benefit a statute has been enacted; (2) that a private right of action would promote the legislative purpose behind the statute; and (3) that creation of the right would be consistent with the overall legislative scheme." *Fagan v. AmerisourceBergen Corp.*, 356 F. Supp. 2d 198, 214 (E.D.N.Y. 2004). Plaintiffs here have met each of these requirements to impose negligence per se.

GEICO violated both the FTC Act and the GBL by failing to enact reasonable security measures to protect Plaintiffs' and class members' highly sensitive personal and driving information. CAC ¶¶ 64-68, 96-101. Both the FTC Act and the GBL were enacted to protect Plaintiffs and their sensitive personal information from exactly the kind of theft and harm they experienced. *See*, *e.g.*, 15 U.S.C. § 15 (the FTC Act's "underlying purpose" is to prevent unfair trade practices which "causes or is likely to cause substantial injury to consumers."); *Corbin v. Wilson*, No. 10-CV-3156 NGG RER, 2011 WL 4374213, at *2 (E.D.N.Y. Aug. 26, 2011) *report and recommendation adopted,* No. 10-CV-3156 NGG RER, 2011 WL 4381152 (E.D.N.Y. Sept. 19, 2011) ("GBL § 349 was intended to protect consumers" from "acts or practices [that] have a broader impact on consumers at large.").

Allowing Plaintiffs to hold GEICO accountable for their negligent failure to implement the safeguards imposed by the FTC Act and GBL would "further [the] policy of protection" envisioned in those statutes. *Lugo v. St. Nicholas Assocs.*, 2 Misc. 3d 212, 216 (Sup. Ct. N.Y. Cnty. 2003)*, aff'd,* 18 A.D.3d 341, 795 N.Y.S.2d 227 (2005). Indeed, federal courts have consistently recognized that the FTC Act can form the basis of a negligence per se claim. *In re Cap. One*, 488 F. Supp. 3d at 407-08 ("[B]ecause New York law would permit the [p]laintiffs to assert a negligence *per se* claim premised on a federal statute and because [p]laintiffs have adequately done

so here—importing the standard of care from the FTC Act—[p]laintiffs have plausibly alleged a claim for negligence *per se* under New York law."); *see also Sanchez v. Ehrlich*, No. 16-CV-8677 (LAP), 018 WL 2084147, at *8 (S.D.N.Y. Mar. 29, 2018) ("[T]he Court finds that Plaintiff alleges sufficiently a statutory duty of care pursuant to N.Y. GBL § 349 sufficient to support a claim of negligence *per se*."); *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 479 (D. Md. 2020); *In re Equifax*, 362 F. Supp. 3d at 1327 (denying motion to dismiss negligence *per se* claim based on a violation of the FTCA); *Bans Pasta, LLC v. Mirko Franchising, LLC*, No. 7-13-cv-00300-JCT, 2014 WL 637762, at *13 (W.D. Va. Feb. 12, 2014) (same).

Whether under the FTC Act or the GBL, GEICO's conduct constitutes negligence *per se*. Thus, this Court should sustain Plaintiffs' negligence per se claim.

V. PLAINTIFFS STATE A GBL § 349 CLAIM

The New York Deceptive Trade Practices Act prohibits "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service." N.Y. Gen. Bus. § 349(a). To assert a viable GBL claim, "a plaintiff must allege that a defendant has engaged in (1) consumer-oriented conduct that is (2) materially misleading and that (3) plaintiff suffered injury as a result of the allegedly deceptive act or practice." *Cohen v. Ne. Radiology, P.C.*, No. 20-cv-1202-VB, 2021 WL 293123, at *9 (S.D.N.Y. Jan. 28, 2021) (quoting *Orlander v. Staples, Inc.*, 802 F.3d 289, 300 (2d Cir. 2015)). Plaintiffs' allegations satisfy each element.

Plaintiffs have alleged that Defendants provided inadequate security to Plaintiffs' New York driver's license numbers, enabling criminals to submit fraudulent unemployment applications in Plaintiffs' names to the state of New York. Defendants argue that their misconduct is insufficiently linked to New York for that state's law to apply, but this argument is misplaced because this case is not a traditional fraud case. MTD at 33-34. Here, Plaintiffs are not alleging

that Defendants fraudulently induced them into a transaction in New York; instead, they are alleging that Defendants engaged in deceptive and fraudulent courses of action while doing business in New York, and while holding and failing to protect the PI of New York residents. That is more than sufficient to establish the required nexus.

Further, Plaintiffs allege that GEICO engaged in consumer-oriented conduct by selling insurance policies to consumers. CAC ¶¶ 4, 50, 140. In doing so, GEICO engaged in deceptive, unfair, and unlawful acts by, among other things, implementing an auto-populate feature into its website to generate insurance policies during a time of heightened cybercriminal activity specifically targeting driver's license numbers and failing to develop reasonable safeguards to protect this information despite its express representations to the contrary. *Id*. ¶¶ 6-9, 77-78, 155-162. As a result of this conduct, Plaintiffs were harmed by identity theft, fraudulent unemployment and insurance claims filed in their names, and fraudulent charges to their financial accounts, requiring substantial time and effort to remediate. *Id*. ¶¶ 18-26, 31-37, 42-47, 167.

While a plaintiff must "show that the material deceptive act caused the injury" it "need not plead or allege reliance." *Doe v. Uber Techs., Inc.*, 551 F. Supp. 3d 341, 372 (S.D.N.Y. 2021); *Bell v. Gateway Energy Services Corp.*, No. 031168/2018, 2021 WL 1151179, at *7 (N.Y. Sup. Ct. Jan. 8, 2021) (finding that "reliance is not an element of a section 349 claim, and section 349 contains no requirement that an injured party show reasonably reliance on erroneous statements . . . in order to obtain relief") (internal quotations omitted).

Courts within the Second Circuit have previously held that a plaintiff adequately plead causation under § 349 when a defendant's failure to disclose "purportedly inadequate data security measures would mislead a reasonable consumer." *Cohen*, 2021 WL 293123, at *9 (internal citations omitted); *see also Fero v. Excellus Health Plan Inc.*, 236 F. Supp. 3d 735, 776-77

(W.D.N.Y. 2017), *on reconsideration*, 304 F. Supp. 3d 333 (W.D.N.Y. 2018), *and order clarified*, 502 F. Supp. 3d 724 (W.D.N.Y. 2020) (sustaining the GBL claim). Accordingly, the Court has a sufficient basis to reject GEICO's attempt to manufacture and impose an additional pleading requirement on Plaintiffs at this stage.

As plaintiffs have detailed in Sections I.D and III.B, *supra*, Defendants' conduct caused them injury and damages. Thus, the Court should allow Plaintiffs' GBL claim to survive at the pleading stage. *See*, *e.g., In re Cap. One*, 488 F. Supp. 3d at 426; *In re Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 996 (N.D. Cal. 2016).

VI. PLAINTIFFS ARE ENTITLED TO DECLARATORY AND INJUNCTIVE RELIEF

Plaintiffs incorporate and reallege the allegations and arguments made to address traceability and redressability with regarding to Article III standing. *See* Section I.D, *supra*. While Plaintiffs do not know the full extent of the Data Disclosure without the benefit of discovery, there is no indication that GEICO has rectified the shortcomings in its system to prevent further disclosure of Plaintiffs' and class members' personal information, which GEICO still collects and stores. Further, Plaintiffs note that GEICO has not sufficiently notified Plaintiffs and class members of the full extent of the Data Disclosure. CAC ¶¶ 70, 202-206. Thus, contrary to GEICO's arguments, Plaintiffs state a claim for declaratory judgment based on the continued risk that their sensitive information is acquired and misused by unauthorized persons. The Southern District of New York agreed with Plaintiffs' argument based on substantially similar factual allegations:

> To seek relief under the Declaratory Judgment Act, a plaintiff must adequately allege a dispute that is: (1) "definite and concrete, touching the legal relations of parties having adverse legal interests"; (2) "real and substantial"; and (3) "admit[ting] of specific relief through a decree of a conclusive character, as distinguished from an opinion advising what the law would be upon a hypothetical state of facts." *MedImmune, Inc. v. Genentech, Inc.*, 549 U.S. 118, 127 (2007) (analyzing 28 U.S.C. § 2201).

> Here, plaintiffs plead an ongoing, actionable dispute arising out of USAA's allegedly inadequate data-security measures, including its fraud-detection capabilities and its pre-filling of driver's license numbers, in breach of its duty of care.

In re USAA, 2022 WL 3348527, at *11–*12. (citing *In re Cap. One*, 488 F. Supp. 3d at 414–15 (plaintiff sufficiently alleged declaratory judgment claim in data-breach case even when defendant allegedly disclosed it corrected the alleged vulnerability)).

Additionally, Plaintiffs are entitled to injunctive relief because on the same allegations that show that "monetary damages, are inadequate to compensate for th[e] injury." *In re USAA*, 2022 WL 3348527, at *11-*12 (finding that "plaintiffs plausibly allege entitlement to the injunctive relief it seeks in conjunction with its request for a declaratory judgment"); *see also In re Cap. One*, 488 F. Supp. 3d at 414–15 (plaintiff sufficiently alleged declaratory judgment claim in data-breach case even when defendant allegedly disclosed it corrected the alleged vulnerability). Thus, Plaintiffs' claim for declaratory judgment and injunctive relief is not subject to dismissal.

VII. CONCLUSION

For the reasons discussed above, Plaintiffs respectfully request that the Court deny GEICO's motion to dismiss in its entirety.

Dated: October 5, 2022

Respectfully submitted,

/s/ Tina Wolfson

TINA WOLFSON (NY Bar No. 5436043)
DEBORAH DE VILLA (NY Bar No. 5724315)
AHDOOT & WOLFSON, PC
100 Avenue of the Americas, 9th Floor
New York, NY 10013
Telephone: (917) 336-0171
Facsimile: (917) 336-0177
twolfson@ahdootwolfson.com
ddevilla@ahdootwolfson.com

ROBERT AHDOOT
(admitted *pro hac vice*)
AHDOOT & WOLFSON, PC
2600 W. Olive Avenue, Suite 500
Burbank, CA 91505
Telephone: (310) 474-9111
Facsimile: (310) 474-8585
rahdoot@ahdootwolfson.com

Dated: October 5, 2022

/s/ E. Michelle Drake

E. MICHELLE DRAKE
(admitted *pro hac vice*)
JOSEPH C. HASHMALL
(admitted *pro hac vice*)
BERGER MONTAGUE PC
1229 Tyler Street NE, Suite 205
Minneapolis, MN 55413
Telephone: (612) 594-5999
Facsimile: (612) 584-4470
emdrake@bm.net
jhashmall@bm.net

Interim Co-Lead Class Counsel

Dated: October 5, 2022

/s/ Karen Hanson Riebel

KAREN HANSON RIEBEL
(admitted *pro hac vice*)
KATE M. BAXTER-KAUF
(admitted *pro hac vice*)
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Avenue South, Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
Facsimile: (612) 339-0981
khriebel@locklaw.com
kmbaxter-kauf@locklaw.com

Additional Counsel for Plaintiffs